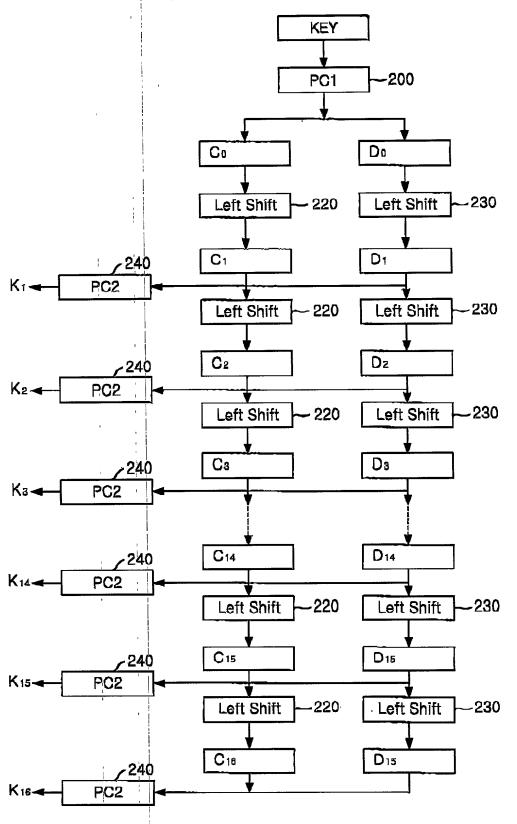
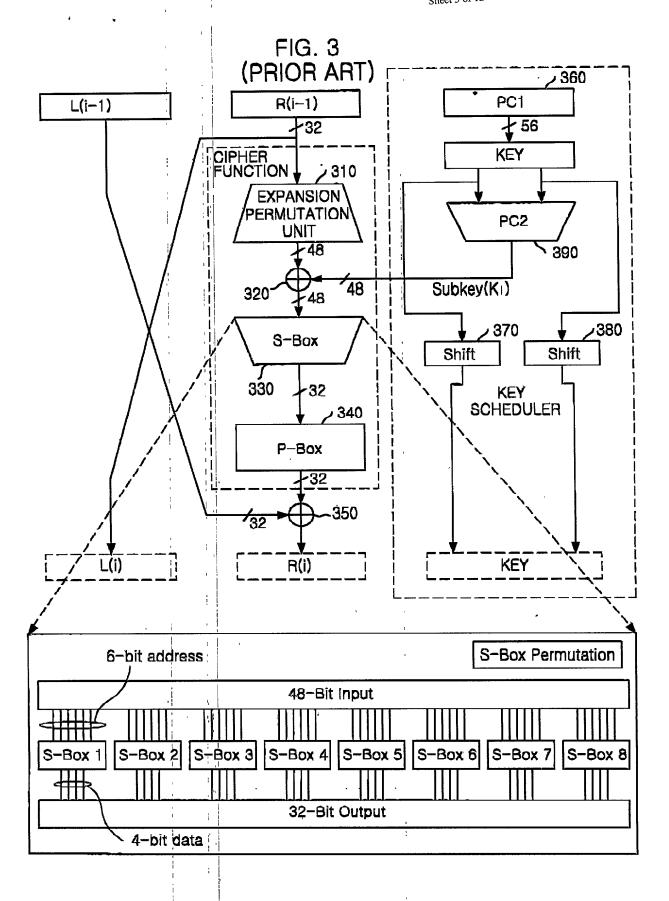
Inventor: LIM Filing Date: June 12, 2001 Attorney Docket: 281196 Sheet 1 of 12 FIG. 1 (PRIOR ART) **PLAIN TEXT** -110 IΡ Ro Lo K₁ 121 -120 122 $R_1 = L_0 \oplus f(R_0, K_1)$ $L_1 = R_0$ K٤ 121 122 R2 =L1 @f(R1, K2) L2 = R1 Ks 121-122 $R_3 = L_2 \oplus f(R_2, K_8)$ $L_3 = R_2$ R₁₄=L₁₃⊕ f(R₁₃, K₁₄) L14= R13 K₁₅ 121 122 R15=L149 f(R14, K15) L₁₅ = R₁₄ Kie 121 R16=L15 + f(R15, K16) L16 - R15 -130 IP **CIPHER TEXT**

Inventor: LIM Filing Date: June 12, 2001 Attorney Docket: 281196 Sheet 2 of 12

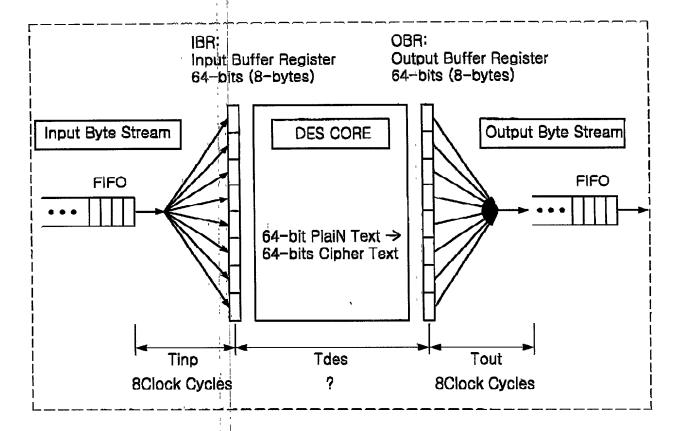
FIG. 2 (PRIOR ART)

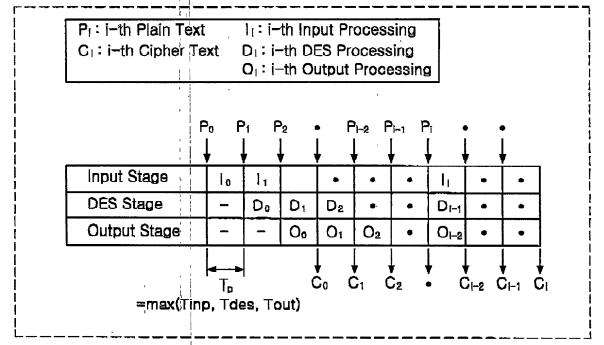




Inventor: LIM Filing Date: June 12, 2001 Attorney Docket: 281196 Sheet 4 of 12

FIG. 4 (PRIOR ART)





Inventor: LIM Filing Date: June 12, 2001 Attorney Docket: 281196 Sheet 5 of 12

FIG. 5A (PRIOR ART)

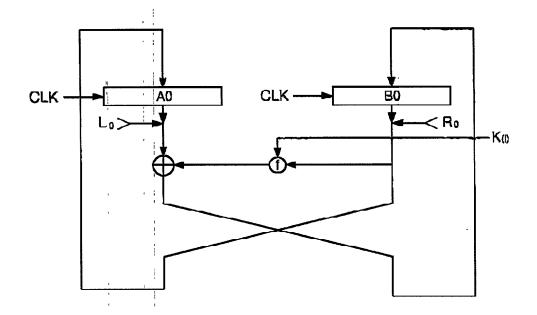


FIG. 5B

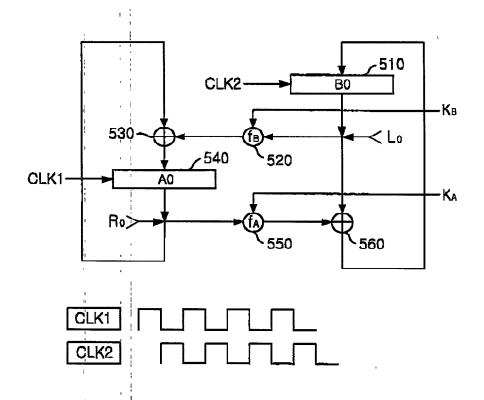
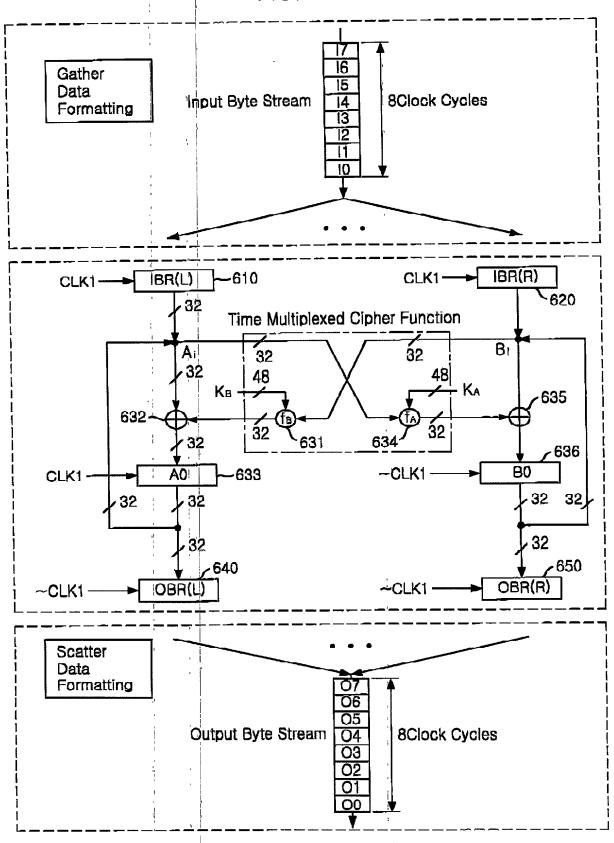


FIG. 6



Inventor: LIM Filing Date: June 12, 2001 Attorney Docket: 281196 Sheet 7 of 12 FIG. 7 K_{B} Bı KA TIME MULTIPLEXED CIPHER FUNCTION fв Kв KA Bı 132 720 -710 **EXPANSION EXPANSION** PERMUTATION PERMUTATION **UNIT** UNIT 48 -48 48 -48 730 48 48 750 MULTIPLEXER **∤**48 760 S-Box **PERMUTATION UNIT** 132 - 770 P-Box PERMUTATION UNIT -780 DE-Select -MULTIPLEXER 32

fe

-	·
Total Shift Amount 2 6 10 17 17 21 25 0	Unit 2 8 rounds 8 rounds 1 40 1
Left Shiff Amount 4 4 4 4 4 4 4 4 2 3	Che
Hound 1(Q ₀) 2(Q ₁) 3(Q ₂) 4(Q ₃) 6(Q ₅) 7(Q ₆) 8(Q ₇)	8 rounds
Total Shift Amount 4 8 12 15 15 19 23 27 TIME, IT SHOULD BE 1	800 B00 DA 720 DA 740 Spunou 8
Round Left Shift Amount Total Shift Amount 1(Po) 3 1 2(P1) 4 4 3(P2) 4 8 4(P3) 3 12 5(P4) 4 15 6(P5) 4 19 7(P6) 4 19 7(P6) 4 23 8(P7) 2 27 WHEN KEY IS LOADED FIRST TIME, IT SHOULD BE 27	710 Key Key CLK1 CLK1 CLK1 PC1 PC1 PC1 PC1 PC1 PC1 PC1 PC2
© © — [4] = [4]	8 rounds

Inventor: LIM Filing Date: June 12, 2001 Attorney Docker: 281196 Sheet 8 of 12

FIG. 9

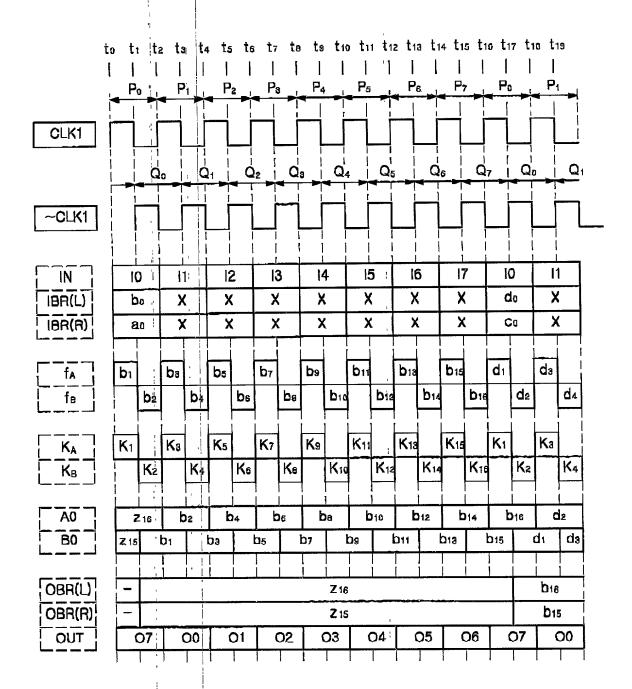
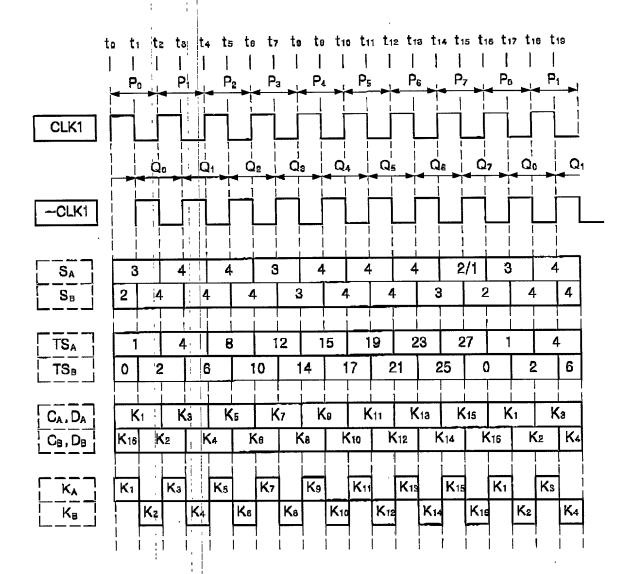
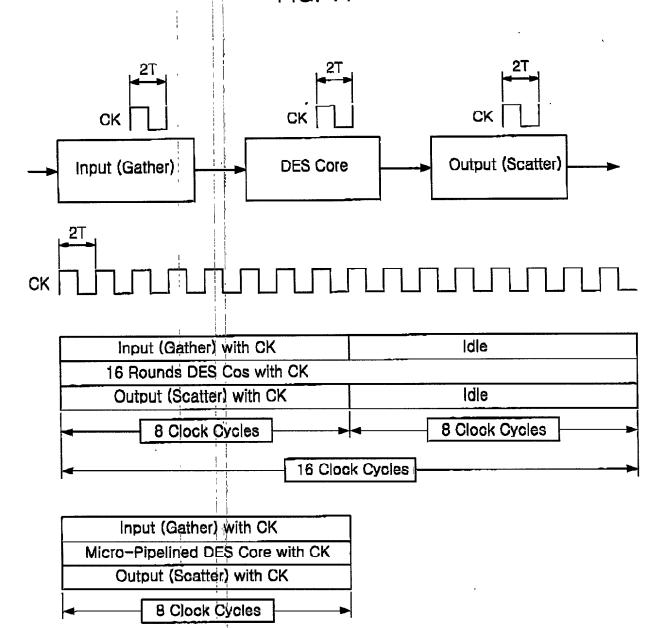


FIG. 10



Inventor: LIM Filing Date: June 12, 2001 Attorney Docket: 281196 Sheet 11 of 12

FIG. 11



Inventor: LIM Filing Date: June 12, 2001 Attorney Docket: 281196 Sheet 12 of 12

FIG. 12

